UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,661	04/02/2004	Marufa Kaniz	AMDP763US	1039

90237 7590 11/16/2009

Eschweiler & Associates, LLC
629 Euclid Avenue
Suite 1000
Cleveland, OH 44114

EXAMINER	
BAYOU, YONAS A	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
11/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/816,661	KANIZ ET AL.	
	Examiner	Art Unit	
	YONAS BAYOU	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-12 and 14-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-12 and 14-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04/02/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's response filed on 07/23/2009.

2. Claims 1-6, 8-12 and 14-23 are pending.

3. Claims 7 and 13 are cancelled.

4. Applicant's arguments have been fully considered.

Response to Arguments

1. Applicant, on pages 7-9, of the remarks, argues "Either Yang or Cheng do not teach a system, wherein the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system."

Examiner respectfully disagrees and asserts that Cheng discloses as illustrated in FIG. 4, SU.sub.k 105, upon receiving a SA request message from SU.sub.k+1 110, as indicated by the directional arrow marked "2" sends a reply message 405 to SU.sub.k+1 110, wherein the reply message 405 contains the information necessary to define the ISAKMP SA attributes identified above in FIG. 3, and the information necessary to define the following IP.sub.SEC SA attributes **[6:45 – 7:6 and fig. 4].** In a first phase (i.e., phase 1), the communicating parties negotiate the ISAKMP SA. The ISAKMP SA is defined by a set of basic security attributes which provide protection for subsequent ISAKMP exchanges. In a second phase (i.e., phase 2), and under the

protection of the ISAKMP SA, the communicating parties negotiate the IP.sub.SEC SAs associated with the IP.sub.SEC authentication header (AH) protocol and/or the IP.sub.SEC encapsulating security payload (ESP) protocol. The IP.sub.SEC protocols provide security services for communications at the IP layer. As is known in the art, a specific IP.sub.SEC SA is uniquely defined by a security parameter index (SPI), a destination IP address, and an IP.sub.SEC protocol (i.e., AH or ESP) **[1:30-60 and fig. 4;** encryption can be done prior to establishing phase II/IP SEC SA attributes].

2. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims as follows:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-6, 8-12 and 14-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yang et al. Patent Number 7,003,118 B1 in view of Cheng et al., Patent No.: US 6,418,130 B1.

Referring to claims 1, 10-11, 15 and 23, Yang teaches a network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising:

a bus interface system adapted to be coupled with a host bus in the host system and transfer data between the network interface system and the host system **[2:37-45];**

a media access control system adapted to be coupled with the network and to transfer data between the network interface system and the network **[1:43-60;** firewall equates MAC system inside NIC];

a memory system coupled with the bus interface system and the media access control system, the memory system being adapted to store incoming and outgoing data being transferred between the network and the host system **[3:5-43, fig. 1A (buffer 150) and fig. 1B (buffer 151)]**;

a security system coupled with the memory system, the security system being adapted to selectively encrypt outgoing data and to selectively decrypt incoming data **[3:5-43, fig. 1A (state machine 155) and fig. 1B (state machine 156)]**; and Yang further teaches: a descriptor management system coupled with the bus interface system and the security system, the descriptor management system being adapted to obtain initialization vector information from the host system and to provide the initialization vector information to the security system **[6:49-65 and fig. 3]**. Yang does not appear to explicitly teach a system, wherein the security system is adapted to employ an initial

random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system. However, Cheng teaches in FIG. 4 illustrates the SA attributes that might be transferred from SU.sub.k 105 to SU.sub.k+1 110, in addition to the SA attributes identified in FIG. 3, if the full SA reuse embodiment is employed. As illustrated in FIG. 4, SU.sub.k 105, upon receiving a SA request message from SU.sub.k+1 110, as indicated by the directional arrow marked "2" sends a reply message 405 to SU.sub.k+1 110, wherein the reply message 405 contains the information necessary to define the ISAKMP SA attributes identified above in FIG. 3, and the information necessary to define the following IP.sub.SEC SA attributes: the IP.sub.SEC SA lifetime; the IP.sub.SEC protocols being used, that is, the authentication header and/or encapsulating security payload protocols; the IP.sub.SEC protocol mode, that is, the transport mode or the tunnel mode; the security parameter index(es); the IP.sub.SEC session keys, including the session keys for authentication and encryption, as well as their respective algorithms; the last CBC output block prior to hand-over, which is used as the initialization vector for encryption of the first IP packet subsequent to hand-over; and the value of the sequence number, in accordance with the authentication header protocol or the encapsulating security payload protocol, just prior to hand-over, as this value plus 1 will be the initial value of the sequence number after hand-over for anti-relay checking purposes. As was the case in FIG. 3, the transfer of SA attributes in FIG. 4 is accomplished in accordance with the direct transfer technique described above. However, it will be understood that the SA attributes may be transferred in accordance with the intermediate storage technique **[6:45 – 7:6, 1:30-**

60, and fig. 4; "the last CBC output block prior to hand-over which is used as an initialization vector for the encryption of the first IP packet subsequent to hand-over"]. Yang and Cheng are analogous art because both teach encryption operation.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the method of Yang to include the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system of Cheng because a mobile unit can begin secure communications immediately following the hand-over [abstract], please see KSR International Co. v. Teleflex Inc., 550 U.S-, 82 USPQ2d 1385 (2007) for further interpretation.

Referring to claim 2, Yang teaches a network interface system, wherein the security system comprises at least one transmit security processor adapted to selectively encrypt or selectively authenticate the outgoing data **[3:5-43 and fig. 1B].**

Referring to claims 3 and 9, Yang as modified teaches a network interface system, wherein the initialization vector information indicates whether the outgoing data is to undergo cipher block chaining (CBC) encryption in the security system **[Cheng: 6:26-67 and figs. 3-4]**.

Referring to claims 4, 5, 17 and 20, Yang as modified teaches a network interface system, wherein the at least one transmit security processor selectively

employs an initialization vector (IV) comprising the initial random data string from the outgoing data to perform CBC encryption according to the initialization vector information from the descriptor management system **[Cheng: 6:26-67 and figs. 3-4]**.

Referring to claims 6, 8, 12, 14, 18, 19, 21 and 22, Yang teaches a network interface system, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data **[5:52-57].**

Referring to claim 16, Yang teaches a method of encrypting outgoing data in a network interface system, wherein providing the initialization vector information comprises:

reading a transmit descriptor from a host system **[5:52-57]**; and

providing initialization vector information from the transmit descriptor to the security system **[5:52-57, 7:50-63 and fig. 4]**.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YONAS BAYOU whose telephone number is (571)272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yonas Bayou/

Examiner, Art Unit 2434

11/10/2009

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434